EMBEDDING A UNQUE SERIAL NUMBER INTO THE CONTENT OF AN EMAIL FOR TRACKING INFORMATION DISPERSION

BACKGROUND

[0001] 1. Field of the Invention

[0002] The present invention relates to the field of email tracking and, more particularly, to embedding a unique serial number into the content of an email for tracking information dispersion.

[0003] 2. Description of the Related Art

[0004] In business today, email is commonly used to communicate with a business' employees. Often these emails contain sensitive information that is not intended for public consumption. Many problems could arise for a business if such sensitive information was leaked. For example, an email could contain information regarding a new line of products in development by the company. If this information was leaked to a competitor for example, this could give the competitor the chance to come up with a better product before the product is even released.

[0005] Currently, protection exists to keep a user from copying sensitive information, but these protections can easily be circumvented. For example, a user can take screenshots of the information, or copy them to a USB drive to prevent firewall based tracking. The user can then disperse the sensitive information to whoever they want. There are currently solutions for tracking down such information leaks. For example, one such solution is called a "canary trap" where the contents can be modified in each email and sent to a unique user, associating a revision of the content with the recipient user. When a leak occurs, the leaked text can be referenced to the user to find the source of the leak. The problem with implementing such a system is that a user has to manually do these modifications and track the changes with their associated users. This kind of implementation becomes very troublesome with a large number of recipient users. A more intuitive solution is required to track information dispersion in emails.

SUMMARY OF THE INVENTION

[0006] The present invention can allow for embedding a unique serial number into the content of an email for tracking information dispersion. This can allow a similar solution such as a "canary trap" to work on a much larger scale to track information dispersion. The present invention can allow the email author to build a serial number system into their email. A serial number can be embedded into email content by strategically changing words in the email content with synonyms. Each word replacement can have an associated bit flag or value. When all of the text replacements are processed together, their associated value or bit flag can create a unique serial number. In one embodiment, the replacements can occur at the client-side based upon substitutions defined in a unique, possibly encrypted header that is included with each sent message. When a leak occurs, the author can input the leaked text and the application can return the serial number for that revision. The disclosed invention can also allow the option to build in redundancy checking in the event a portion of the document is quoted. This also allows for the assignment of a serial number based on department. This can prevent two users from noticing a difference between emails sent to them and someone else in their department. The serial number can also include a CRC (Cyclic Redundancy Code) number or modulus check. This can prevent a recipient from noticing the serial number and attempting to change the number and potentially picking the wrong person as the source of the leak.

[0007] Another aspect of the present invention can include a user interface for configuring the embedded serial numbers and tracking them. One such user interface can allow a user to establish and identify interchangeable words in the email. Synonyms for these interchangeable words can be retrieved from a thesaurus and displayed for the user, which can allow the user to select which words to use for substitution. The present invention can also allow for random generation of email content with embedded serial numbers. A user can preview the generated revisions of the email content with embedded serial numbers for clarity, to make sure the initial content is still intact, before assigning each revision to a department, user, company, or the like. Serial numbers and therefore revisions of the email can be assigned to any distinguishable entity for tracking information dispersion.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] There are shown in the drawings, embodiments which are presently preferred, it being understood, however, that the invention is not limited to the precise arrangements and instrumentalities shown.

[0009] FIG. **1** is a schematic diagram of a system for embedding a unique serial number into the content of an email for tracking information dispersion in accordance with an embodiment of the inventive arrangements disclosed herein.

[0010] FIG. **2** illustrates a system of sample user interfaces for embedding a unique serial number into the content of an email for tracking information dispersion in accordance with an embodiment of the inventive arrangements disclosed herein.

[0011] FIG. **3** illustrates a system of sample user interfaces for embedding a unique serial number into the content of an email for tracking information dispersion in accordance with an embodiment of the inventive arrangements disclosed herein.

[0012] FIG. **4** is a flow chart of a method for embedding a unique serial number into the content of an email for tracking information dispersion in accordance with an embodiment of the inventive arrangements disclosed herein.

DETAILED DESCRIPTION OF THE INVENTION

[0013] FIG. **1** is a schematic diagram of a system **100** for embedding a unique serial number into the content of an email for tracking information dispersion in accordance with an embodiment of the inventive arrangements disclosed herein. In system **100**, user **102** can generate a series of emails **120** to be sent to recipient users **104**, **106**, **108**, **109** with embedded serial numbers for tracking information dispersion. The serial number can be hidden in email content through a series of equivalent word substitutions. User **102** can interact with an email client running on computing device **110** to create the emails to be sent. Computing device **110** can interact with mail server **150** through network **140** to send emails **120**. Emails **120** can be sent as emails **122**, **124**, **126**, and **128** to user **104**, **106**, **109**, and **108**. Each email **122**-**128** can include a unique serial number that can identify the recipient of the email. Users **104**, **106**, **108**, and **109** can use client **112**, **114**, **116**, and **118** respectively to receive their